

REMARKS

In the Office Action, the Examiner rejected claims 1, 3-20, 22-27, and 29-32. Claims 1, 2, 9, 10, 13, 19, 21, 26, 27, and 28 have been amended. Claims 7, 8, 12, and 20 have been canceled. Claims 1-6, 9-11, 13-19, and 21-32 remain pending. In view of the following remarks, Applicants respectfully request reconsideration and allowance of all pending claims.

Rejections under 35 U.S.C. § 102

The Examiner rejected claims 1, 3-7, 12, 19-20, and 22-24 under 35 U.S.C. § 102(b) as being anticipated by Bruce Schneier's "Applied Cryptography", (hereinafter referred to as "the Schneier reference"); and claims 13-18, 25, 27, and 29-32 under 35 U.S.C. § 102(b) as being anticipated by Utz et al., (U.S. Patent No. 5,680,131, hereinafter referred to as the "Utz reference." Applicants respectfully traverse these rejections.

Legal Precedent

Anticipation under Section 102 can be found only if a single reference shows exactly what is claimed. *Titanium Metals Corp. v. Banner*, 227 U.S.P.Q. 773 (Fed. Cir. 1985). For a prior art reference to anticipate under Section 102, every element of the claimed invention must be identically shown in a single reference. *In re Bond*, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990). To maintain a proper rejection under Section 102, a single reference must teach each and every limitation of the rejected claim. *Atlas Powder v. E.I. du Pont*, 750 F.2d 1569 (Fed. Cir. 1984). The prior art reference also must show the *identical* invention "*in as complete detail as contained in the ... claim*" to support a *prima facie* case of anticipation. *Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989) (emphasis added).

Accordingly, Applicants need only point to a single element not found in the cited reference to demonstrate that the cited reference fails to anticipate the claimed subject matter.

Claim 1-7, 12 and 19-26

Applicants respectfully assert that the Schneier reference does not anticipate independent claims 1 and 19 under Section 102 because not every element of the claimed invention is disclosed. Specifically, claim 1 as amended recites, *inter alia*, a method of generating a cryptographic security subsystem comprising the acts of “(b) writing one or more bits of data to a seed pool upon termination of the first type of triggering event, the seed pool comprising a state bit indicative of a state of the seed pool...(d) writing one or more bits of data to the seed pool upon termination of the second type of triggering event, wherein act (d) comprises masking one or more bits of data to the seed pool upon termination of the second type of triggering event; (e) examining the state bit to determine whether the seed pool is full.” Claim 19 as amended recites, *inter alia*, a communications management subsystem comprising “a non-volatile memory device to store a seed pool, wherein the seed pool comprises a state bit indicative of the state of the seed pool; and security logic...configured to: detect the occurrence of a first type of triggering event; examine the state bit to determine whether the seed pool is fully populated; write one or more bits of data to the seed pool upon termination of the first type of triggering event if the seed pool is not fully populated; detect the occurrence of a second type of triggering event; examine the state bit to determine whether the seed pool is fully populated; and mask one or more bits of data to the seed pool upon termination of the second type of triggering event.”

In contrast, the Schneier reference does not disclose anything with regards to determining if a seed pool is full or the masking of bits into the seed pool. Specifically, the Schneier reference discusses the problem of insufficient randomness. *See* Schneier, p. 428. The Schneier reference explains that if a system reboots without seeing any input there may be insufficient randomness in the Randpool array. *See id.* As a solution, the Schneier reference suggests requiring a user to type after the first reboot to create a seed file which is saved on a disk. *Id.* A potential problem with this approach is that an attacker may steal the seed file between reboots and use it to access the system in the future. *See id.* In order to avoid this problem, the Schneier reference explains that the only solution is to wait for external random events to take place after a reboot before hashing the seed file to produce results. *Id.* The Schneier reference, therefore, discloses nothing more than waiting for external events, writing bits to the seed file, and then hashing the seed file. However, the Schneier reference does *not* disclose a seed pool having a state bit which is used to determine whether the seed pool is full or masking one or more bits into the seed pool as recited in claims 1 and 19. *See id.* As such, the Schneier reference does not anticipate claims 1 and 19.

Accordingly, Applicants request withdrawal of the rejection of claims 1 and 19. Additionally, Applicants request withdrawal of the rejection of all claims dependent from claims 1 and 19, specifically claims 3-7, 20 and 22-26.

Claims 13-18 and 27-32

Applicants respectfully assert that the Utz reference does not anticipate independent claims 13 and 27 because it fails to disclose every element of the claimed invention. As

described in the Application, in a manufacturing environment, a cryptographic security subsystem may hinder the efficient assembly and testing of a device. Application, p. 23, ll. 5-8. Specifically, a manufacturing process may include installation of software and testing which involves establishment of communications between the device via a communications link and power to the device may be cycled several times. *Id.* at ll. 8-11. If the security subsystem has been enabled, then each time power is cycled or the device is rebooted, a secure connection must be established and a technician must then provide a login identifier and password, which may require special knowledge on the part of the technician as well as being time consuming. *Id.* at ll. 11-18. However, the security subsystem must be installed during the manufacturing process to ensure that the device does not leave the manufacturing environment without proper safeguards. *Id.* at ll. 18-22.

To alleviate the concerns regarding the security device and to eliminate inefficiencies in the manufacturing environment, security features are bypassed based on the state of the seed pool. Application, p. 24, ll. 6-9. Specifically, a signature value may be used, wherein as long as the seed pool contains the signature value (or a significant portion of the signature value) the security subsystem is bypassed. *Id.* at ll. 9-14. Every time power is cycled or the system has to reboot, bits are written into the seed pool, thus altering the signature value. *Id.* at ll. 16-20. If security logic determines that more than a threshold number of bits have been altered in the signature value, security features are no longer bypassed.

As such, claim 13 as amended recites, *inter alia*, "A method of initializing a seed pool...comprising the acts of: (a) prior to enabling the cryptographic security subsystem,

writing a plurality of bits of data to a seed pool, the plurality of bits having a signature value...(c) writing one or more bits to the seed pool upon termination of the first type of triggering event, the one or more bits of data altering the signature value of the seed pool; and enabling the cryptographic security subsystem when more than a predetermined portion of the signature value of the seed pool has been altered.” Additionally, claim 27 as amended recites, *inter alia*, “A processor-based device comprising...a non-volatile memory device to store a seed pool comprising a plurality of data bits; and security logic in communication with ... the non-volatile memory device....wherein the security logic is configured to: write the one or more bits to the seed pool, the bits altering a signature value; determine whether a plurality of data bits in the seed pool has at least a portion of the signature value; and disable establishment of the secure communication session if the plurality of data bits has at least a portion of the signature value.”

In contrast, the Utz reference does not disclose altering a signature value as set forth in claims 13 and 19. The Utz reference discloses storing bits that are used as a “start value.” Col. 5, ll. 34-38. The Examiner correlates the “start value” with the signature value of the present claims. Assuming, *arguendo*, even if the start value could be correlated to the claimed signature value, the start value of the Utz reference *never changes* because it is used as an identifying value for a receiver to recognize a remote transmitting device. *See*, col. 6, ll. 65 to col. 7 ll. 18. Furthermore, to preclude alteration of the start value, a disable fuse makes the nonvolatile memory where the start value is stored one-time programmable; thus, the start value is *fixed*. *See* col 8, ll. 58 to col. 9, ll. 4. As such, the Utz reference does not disclose

altering a signature value as set forth in claim 13 and 19. Accordingly, the Utz reference fails to anticipate claims 13 and 27 under Section 102.

For at least the above stated reasons, Applicants respectfully request the withdrawal of the rejection of claims 13 and 27 and further request the withdrawal of the rejection of all claims depending therefrom, specifically, claims 14-18 and 29-32.

Rejections under 35 U.S.C. § 103

In the Office Action, the Examiner rejected claims 8-11 under 35 U.S.C. § 103(a) as being unpatentable over the The Schneier reference reference as applied to claims 1-6, and further in view of Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone's "Handbook of Applied Cryptography", hereinafter referred to as "the Menezes reference." Applicants respectfully traverse this rejection.

By this paper, Applicants have canceled claim 8 and amended claim 1 to include the subject matter of claim 8. As amended, claim 1 recites, *inter alia*, a method of generating a cryptographic security subsystem comprising the acts of " writing one or more bits of data to a seed pool upon termination of the first type of triggering event, the seed pool comprising a state bit indicative of a state of the seed pool." As explained in detail above, the Schneier reference fails to disclose a state bit indicative of the seed pool. The Menezes reference fails to cure this deficiency of the Schneier reference. As such, claim 1 as amended to include the subject matter of claim 8 is not obviated by the Schneier and the Menezes references, either

alone or in combination. Accordingly, Applicants respectfully assert that claim 1 is in condition for allowance, as set forth above.


Furthermore, Applicants respectfully assert that claims 9-11 are allowable based on their dependency from claim 1 because the Menezes reference does not cure the deficiencies described above in regard to the the Schneier reference. For this reason, claims 9-11 are believed to be allowable over the cited references taken alone or in combination with each other. Thus, Applicants respectfully request the withdrawal of the rejection of claims 9-11.

Conclusion

Applicants respectfully submit that all pending claims should be in condition for allowance. However, if the Examiner wishes to resolve any other issues by way of a telephone conference, the Examiner is kindly invited to contact the undersigned attorney at the telephone number indicated below.

Respectfully submitted,

Date: March 28, 2006



Michael G. Fletcher
Reg. No. 32,777
(281) 970-4545

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400